In the first place, the "working hypothesis should read "All persons and entities excluding consumers that participate in an electronic health information exchange network at a local, state, regional or nationwide level, through which individually identifiable electronic health information is stored, compiled, transmitted, or accessed, should be required to meet privacy and security criteria that exceed existing relevant Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rule requirements."

My other comment relates to 4. General Questions, bullet C: "Is there a minimum set of confidentiality, privacy, and security protections that you think everyone should follow, if not HIPAA, what?" That minimum set has yet to be defined. It should be defined on a federal level. It should close the embarrassing gaps in HIPAA. A good starting place is derived from the set of principles crafted by the Patient Privacy Coalition.

- The right to privacy applies to all health information regardless of the source, the form it is in, or who handles it
- Patients have the right to medical privacy
- Patients have the right to opt-in and opt-out of electronic systems
- Patients have the right to segment sensitive information
- Patients have control over who can access their electronic health records
- Audit trails are required for every disclosure of patient information
- Patients must be notified promptly of suspected or actual privacy breaches
- Health information disclosed for one purpose may not be used for another purpose before informed consent has been obtained

- Patients cannot be compelled to share health information to obtain employment, insurance, credit, or admission to schools, unless required by statute
- Employers may not have access to employees' medical records before informed consent has been obtained
- All existing holders of health information must disclose the fact that they hold a patient's health information
- Meaningful penalties and enforcement mechanisms for privacy violations must be enacted whether those violations are detected by patients, advocates, or government regulators

Tom Jones, MD
Chief Medical Officer, Tolven
Sonoma, California
707 695 5712 (mobile)
707 939 7845 (office)

www.tolven.org
www.tolvenhealth.com